PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-291050

(43)Date of publication of application : 19.10.2001

(51)Int.Cl. G06K 7/00
B42D 15/10
G06F 12/14
G06K 7/01
G06K 17/00

(21)Application number : 2000-104594

(22)Date of filing : 06.04.2000

(71)Applicant : NEC INFRONTIA CORP

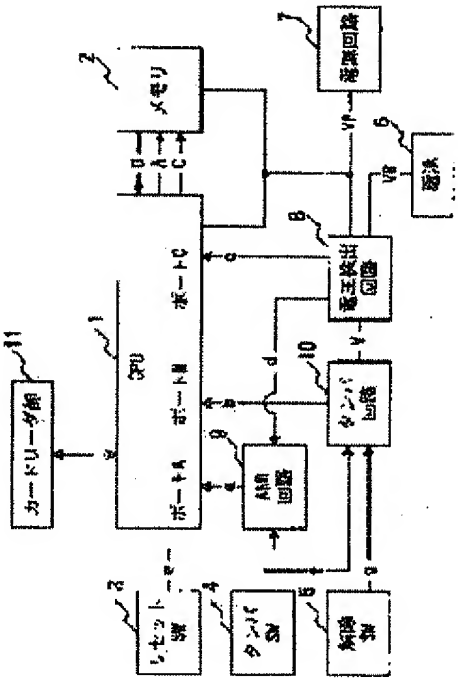
(72)Inventor : ENOMOTO SHIGEHARU

(54) CARD READER PROVIDED WITH SECURITY FUNCTION

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent a card reader from being operated originally when its housing is unpacked and to prevent a data-forged card from being taken out by continuing a disabled state even when the card reader is restored after unpacking.

SOLUTION: The card reader is provided with a CPU 1 for compositely controlling the card reader so as to normally operate a card reader part 11 and a memory 2 is connected to the CPU 1. Also the card reader is provided with a reset SW 3 for resetting a circuit operation, a tamper SW 4 for detecting the unpacking of the device housing and a cancellation switch SW 5 which is a hidden switch. Both power sources of a power circuit 7 and a battery 6 are connected to a voltage detection circuit 8, a battery presence/absence signal (c) and a power supply signal (d) are generated, they are supplied to a port C and the power supply signal (d) and a reset signal (e) are inputted to an AND circuit 9. A temper signal (f) and a cancellation signal (g) are inputted to a tamper circuit 10 and the tamper signal (b) is generated on the basis of both signals and outputted to the port B.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－291050
（P2001－291050A）
(43)公開日　平成13年10月19日(2001.10.19)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　7/00		Ｃ０６Ｋ　7/00	Ｗ	２Ｃ００５
Ｂ４２Ｄ　15/10	５２１	Ｂ４２Ｄ　15/10	５２１	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｃ０６Ｆ　12/14	３２０Ｄ	５Ｂ０５８
Ｇ０６Ｋ　7/01		Ｇ０６Ｋ　7/01	Ｄ	５Ｂ０７２
17/00		17/00	Ｓ	

審査請求　有　請求項の数６　ＯＬ　（全６頁）

(21)出願番号　特願2000－104594(P2000－104594)

(22)出願日　平成12年４月６日(2000.4.6)

(71)出願人　00022/205
エヌイーシーインフロンティア株式会社
神奈川県川崎市高津区北見方２丁目６番１号

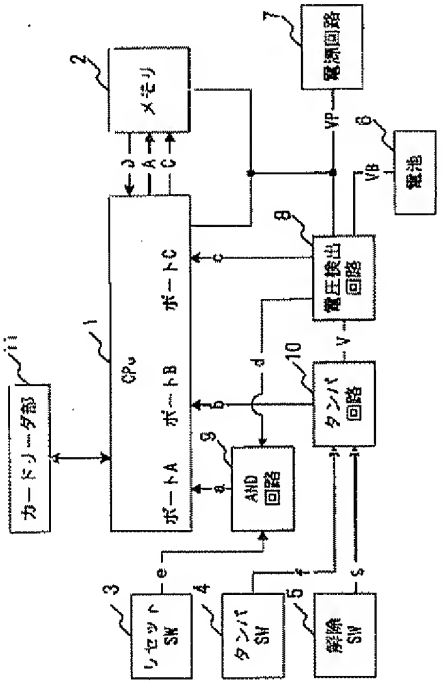
(72)発明者　榎本　茂晴
川崎市高津区北見方２－６－１　日通工株式会社内

(74)代理人　100081710
弁理士　福山　正博

最終頁に続く

(54)【発明の名称】　セキュリティ機能付きのカードリーダ装置

(57)【要約】
【課題】装置筐体に対して開梱が行われた場合に、本来動作を不能にすると共に、開梱後に修復がされても不能状態を継続することによってカード偽造のデータを取り出せなくする。
【解決手段】カードリーダ部１１に対して正規の動作が行われるように複合的に制御するためのＣＰＵ１が設けられ、これにメモリ２が接続される。回路動作をリセットするためのリセットＳＷ３と、装置筐体の開梱を検知するタンパＳＷ４と、隠しスイッチである解除ＳＷ５が設けられる。電源回路７と電池６の両電源は、電圧検出回路８に接続され、電池有／無信号ｃと電源投入信号ｄが生成され、これがポートＣに供給され、電源投入信号ｄとリセット信号ｅがＡＮＤ回路９に入力される。タンパ信号ｆと解除信号ｇは、タンパ回路１０に入力され、両信号に基づいてタンパ信号ｂが生成されてポートＢに出力される。



【特許請求の範囲】
【請求項１】各種情報が記録部に記録されたカードがセットされたときに、該記録部の情報を読み取って外部機器に信号を出力し得るカードリーダ装置において、
前記カードリーダ装置の回路部が収納される装置筐体が開梱されたことを検出した保持信号でなる開梱信号を生成する開梱検出手段と、
前記開梱検出手段によって前記開梱信号が出力されたときに、前記カードリーダ装置に対して所定の動作を行わせるに必要なメモリの格納内容を消去して前記カードリーダー装置の動作を不能にするように制御すると共に、前記装置筐体の開梱が復元されても前記カードリーダー装置の動作を不能にするように制御する制御手段とを具備することを特徴とするセキュリティ機能付きのカードリーダ装置。
【請求項２】各種情報が記録部に記録されたカードがセットされたときに、該記録部の情報を読み取って外部機器に信号を出力し得るカードリーダ装置において、
前記カードリーダ装置の回路部が収納される装置筐体が開梱されたことを検出した保持信号でなる開梱信号を生成する開梱検出手段と、
前記開梱検出手段によって前記開梱信号が出力されたときに、前記カードリーダ装置に対して所定の動作を行わせるに必要なメモリへのアクセスを禁止して前記カードリーダー装置の動作を不能にするように制御すると共に、前記装置筐体の開梱が復元されても前記カードリーダー装置の動作を不能にするように制御する制御手段とを具備することを特徴とするセキュリティ機能付きのカードリーダ装置。
【請求項３】前記開梱検出手段から前記開梱信号が出力されたときに使用不可である旨のエラーメッセージを表示する表示手段を付加して構成することを特徴とする請求項１または請求項２に記載のセキュリティ機能付きのカードリーダ装置。
【請求項４】前記開梱検出手段は、前記装置筐体の開梱によってオンまたはオフするスイッチ部材の出力に基づいて前記開梱信号を生成するように構成することを特徴とする請求項１または請求項２に記載のセキュリティ機能付きのカードリーダ装置。
【請求項５】前記カードは、各種情報が記録部に磁気的に記録された磁気カードで構成されることを特徴とする請求項１ないし請求項４のいずれかに記載のセキュリティ機能付きのカードリーダ装置。
【請求項６】前記カードは、各種情報が記録部に電気的に記録されたＩＣカードで構成されることを特徴とする請求項１ないし請求項４のいずれかに記載のセキュリティ機能付きのカードリーダ装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、各種情報が記録部に記録されたカードがセットされたときに、記録部の情報を読み取って外部機器に信号を出力し得るカードリーダ装置にセキュリティ機能を持たせた「セキュリティ機能付きのカードリーダ装置」に関する。
【０００２】
【従来の技術】クレジットカード、デビットカード、金融機関のキャッシュカード等のカードに記録された情報を読み取って各種の料金支払いを行ったり、関連する各種手続きを行うカードが広く普及していて、ホテル、旅館のキャッシュコーナーやスーパーマーケット等の店舗に設置されカードリーダ装置でその情報を読取り、各種の会計処理を能率的に行うことができる。
【０００３】このカードは、各種情報が記録部に磁気的に記録された磁気カードで構成されたり、各種情報が記録部に電気的に記録されたＩＣカードで構成されている。このようなカードリーダ装置は、通常、独立して設置され、通信回線を介してセンター側のホスト装置に接続されている。
【０００４】このようなカードリーダ装置は、カード利用の普及に伴い、カードデータの読取りを盗み取り（スキミング）、精巧に作られた生のカードに盗み取ったデータを書き込んで偽造カードを作り、本来のカード所有者になりすましてカード利用を行うという不正行為が多発している。特に、クレジットカードは暗証番号入力によるセキュリティがないために容易に偽造カードが利用されてしまう現状にある。
【０００５】かかる不正行為の具体例としては、店舗等に設置してある正規のカードリーダ装置の内部において、記録情報読取り部のコネクタからカード内のデータを横取りするためのスキミング装置を深夜等の不在時に不法侵入して埋め込む方法がある。このときにはカードリーダ装置は正常に動作しているので、カードリーダ装置の管理者は勿論のこと正規のカード所有者も気が付かない内にデータがスキミング装置にデータ格納されるのである。
【０００６】そして、後日に盗み取ったデータをスキミング装置ごと回収し、不正に作られた生のカードに盗み取ったデータを書き込んで偽造カードを作り、本来のカード所有者になりすましてカード利用を行うのである。
【０００７】このような不正を防止するために、次のような方策が提案されている。即ち、カードリーダ装置の装置筐体が開梱されたことを検出するスイッチ部材を設け、このスイッチ作動に伴って、メモリへの電源供給を断ったり、メモリのデータを消去したり、正規の動作プログラムを解読困難とするような変更を行ったり、メモリのアドレスバスの接続を意図的に不規則にすることによって、正規のカードリーダ装置の持っている動作が行えないようにしている（例えば、特開昭６０－４８５５５、特開平１１－１７５４０６参照）。
【０００８】また、装置筐体を組み立てるためのねじに

特殊な治具を用いなければ緩められないような特殊ねじを用いることによって開梱を難しくしたり、装置筐体の接合部を接着して開梱を不可能にしたり、装置筐体の接合部に一度剥がすと元の状態には戻せない特殊シールを貼ることによって不正に開梱されたことが明瞭に判るようにしている。

【0009】

【発明が解決しようとする課題】従来のカードリーダ装置は、装置筐体が不正に開梱された後に、その修復が行われた場合には、カードリーダ装置そのものが正常に動作してしまうので不正な改造が行われたことを外観上で判別することができない場合が多いという問題がある。

【0010】そこで、本発明は、カードリーダ装置の装置筐体に対して開梱が行われた場合に、カードリーダ装置そのものの本来動作を不能にすると共に、開梱の後に修復がなされても本来動作の不能状態を継続することによって開梱されたことを当該機器の管理者や正規のカード利用者に知らしめることによってカードの偽造をできなくするというセキュリティ機能付きのカードリーダ装置を提供することにある。

【0011】

【課題を解決するための手段】前述の課題を解決するために、本発明によるセキュリティ機能付きのカードリーダ装置は、次に記載するような特徴的な構成を採用している。

【0012】（1）各種情報が記録部に記録されたカードがセットされたときに、該記録部の情報を読み取って外部機器に信号を出力し得るカードリーダ装置において、前記カードリーダ装置の回路部が収納される装置筐体が開梱されたことを検出した保持信号でなる開梱信号を生成する開梱検出手段と、前記開梱検出手段によって前記開梱信号が出力されたときに、前記カードリーダ装置に対して所定の動作を行わせるに必要なメモリの格納内容を消去して前記カードリーダー装置の動作を不能にするように制御すると共に、前記装置筐体の開梱が復元されても前記カードリーダー装置の動作を不能にするように制御する制御手段とを具備するセキュリティ機能付きのカードリーダ装置。

【0013】（2）各種情報が記録部に記録されたカードがセットされたときに、該記録部の情報を読み取って外部機器に信号を出力し得るカードリーダ装置において、前記カードリーダ装置の回路部が収納される装置筐体が開梱されたことを検出した保持信号でなる開梱信号を生成する開梱検出手段と、前記開梱検出手段によって前記開梱信号が出力されたときに、前記カードリーダ装置に対して所定の動作を行わせるに必要なメモリへのアクセスを禁止して前記カードリーダー装置の動作を不能にするように制御すると共に、前記装置筐体の開梱が復元されても前記カードリーダー装置の動作を不能にするように制御する制御手段とを具備するセキュリティ機能付きのカードリーダ装置。

【0014】（3）前記（1）または前記（2）の開梱検出手段から前記開梱信号が出力されたときに使用不可である旨のエラーメッセージを表示する表示手段を付加して構成するセキュリティ機能付きのカードリーダ装置。

【0015】（4）前記（1）または前記（2）の開梱検出手段は、前記装置筐体の開梱によってオンまたはオフするスイッチ部材の出力に基づいて前記開梱信号を生成するように構成するセキュリティ機能付きのカードリーダ装置。

【0016】（5）前記（1）ないし前記（4）のいずれかのカードは、各種情報が記録部に磁気的に記録された磁気カードで構成されるセキュリティ機能付きのカードリーダ装置。

【0017】（6）前記（1）ないし前記（4）のいずれかのカードは、各種情報が記録部に電気的に記録されたＩＣカードで構成されるセキュリティ機能付きのカードリーダ装置。

【0018】

【発明の実施の形態】以下、本発明の一実施の形態について図面を用いて詳細に説明する。この形態は、カードが磁気カードの場合であり、先ず、本発明によるセキュリティ機能付きのカードリーダ装置の概略回路構成を示す図１を用いて説明する。

【0019】カードリーダ部１１に対して正規の動作が行われるように複合的に制御するためのＣＰＵ１が設けられ、これにメモリ２が接続されている。この両者間は、書き込みデータと読み出しデータのバスであるデータバスＤと、メモリアドレスを特定するためのアドレスバスＡと、これらを制御するための制御信号Ｃのラインで結合されている。

【0020】また、回路動作をリセットするためのリセットＳＷ３と、装置筐体の開梱を検知するタンパＳＷ４と、隠しスイッチである解除ＳＷ５が設けられ、メモリ２のデータのバックアップ用の電池電源ＶＢを出力する電池６と、商用電源等の出力を整流、安定化した直流でなる主電源ＶＰを出力する電源回路７が設けられている。

【0021】この電源回路７の主電源ＶＰは、ＣＰＵ１とメモリ２に接続され、ＣＰＵ１動作とメモリ２動作が正規に行えるようにされている。また、電源回路７の主電源ＶＰと電池６の電池電源ＶＢの両電源は、電圧検出回路８に接続され、電圧検出回路８によって電池有／無信号ｃと電源投入信号ｄが生成され、電池有／無信号ｃがＣＰＵ１のポートＣに供給され、電源投入信号ｄが２入力型のＡＮＤ回路９の一方の入力端に入力され、ＡＮＤ回路９の他方の入力端には、リセットＳＷ３から出力されるリセット信号ｅが入力される。このＡＮＤ回路９の出力であるハードウエアのリセットを行うためのハー

ド・リセット信号ａは、ＣＰＵ１のポートＡに出力される。

【００２２】また、タンパＳＷ４から出力されるタンパ信号ｆと、解除ＳＷ５から出力される解除信号ｇは、タンパ回路１０に入力され、両信号の相関に基づき生成されたタンパ信号ｂがＣＰＵ１のポートＢに出力される。

【００２３】従って、正規の状態においては、電源投入後、またはハード・リセット信号ａの解除後にＣＰＵ１は、ポートＡ、Ｂ、Ｃの状態を検知していて、装置筐体が不正者によって開梱されると、図２に示すフローチャートのように、先ず、ステップＳ１にてリセットＳＷ３とタンパＳＷ４のそれぞれがオンされるために、リセット信号ｅが立ち上げられＡＮＤ回路９のハード・リセット信号ａが立ち上げられＣＰＵ１のポートＡに供給される。これと同時的に、ステップＳ２にてＣＰＵ１からの指令でメモリ２の格納データが消去され、ＣＰＵ１の動作が停止される。

【００２４】次に、ステップＳ３にてリセットＳＷ３が戻されたか否かが判定され、Ｎｏの場合には待機状態とされ、Ｙｅｓになったときに次のステップＳ４に進み、ステップＳ４にてタンパＳＷ４が戻されたか否かが判定され、Ｎｏの場合には待機状態とされ、Ｙｅｓになったときに次のステップＳ５に進む。

【００２５】ここで、タンパＳＷ４は、一旦オンになるとタンパ信号ｆはアクティブ状態を保持しているので、ステップＳ５にてＣＰＵ１が起動状態にされ、ポートＢ、Ｃが検知され次のステップＳ６にてポートＢがアクティブであるか否かが判定され、Ｎｏの場合には待機状態とされ、Ｙｅｓになったときに次のステップＳ７にてメッセージＡが図示しない表示器や治具等に表示され、この具体例は、図３に符号１２で示すように「システムエラー　Ｓ００１」なる文字表示と「動作不可」なる文字表示である。

【００２６】このような状態を復旧するには、装置筐体の内部に設けられた隠しスイッチである解除ＳＷ５を操作することによって解除信号ｇを立ち上げこれに伴ってタンパ信号ｂがＣＰＵ１のポートＢに供給されることによって実行される。

【００２７】さて、電池６が取り外されると、図４に示すフローチャートのように、先ずステップＳ８にてＣＰＵ１のポートＣがアクティブであるか否かが判定され、Ｎｏの場合には待機状態とされ、Ｙｅｓになったときに次のステップＳ９にてメッセージＢが図示しない表示器や治具等に表示され、これ以後の操作を受け付けないようにされる。このメッセージＢの具体例は、図５に符号１３で示すように「システムエラー　Ｓ００２」なる文字表示と「バックアップ電池切れです。」なる文字表示である。

【００２８】ただし、外した電池６を元に戻せば（ステップＳ１０）、ステップＳ１１にてメッセージＢの表示が解除され、前述のような「操作を受け付けない」状態が解除され、次のステップＳ１２に進んで、タンパＳＷ４がオンされているか否かが判定され、Ｎｏの場合には前述のステップＳ８に戻され、ステップＳ８から先のステップが実行され、ステップＳ１２でＹｅｓになったときに次のステップＳ１３にてメッセージＡ（図３の符号１２参照）が図示しない表示器や治具等に表示され、これ以後の操作を受け付けなくなる。

【００２９】従って、装置筐体を開梱してスキミング装置を搭載してデータ盗用をしようとしても、当該機器を取り外した時点で動作不能状態にされ、しかもこの状態が開梱復旧されても継続して維持されるので、別段に複雑な構成を用いることなくデータ盗用を防止できる。

【００３０】なお、リセットＳＷ３、タンパＳＷ４の具体構成としては、マイクロスイッチの場合のみならず、磁気感知スイッチとして構成されるリードスイッチや半導体スイッチで構成するようにしても良い。

【００３１】また、本発明に用いられるカードは、各種情報が記録部に磁気的に記録された磁気カードの場合のみならず、各種情報が記録部に電気的に記録されたＩＣカードで構成される場合であっても良く、情報の記録の形式は全くの任意であって、当該カードリーダ装置の設置される場所も全くの任意である。

【００３２】さらに、開梱時に動作不能にする手段は、所期の動作を行わせるに必要なメモリの格納内容を消去する例のみならず、カードリーダ装置に対して所定の動作を行わせるに必要なメモリへのアクセスを禁止して前記カードリーダー装置の動作を不能にするように制御したり、所定のプログラム実行を不可能にするようにしても良いことは勿論である。

【００３３】

【発明の効果】以上の説明で明らかなように、本発明によるセキュリティ機能付きのカードリーダ装置は、カードリーダ装置に対して所定の動作を行わせるに必要なメモリの格納内容を消去して前記カードリーダー装置の動作を不能にするように制御し、しかもこの状態を開梱修復があっても継続して保持されるので、装置筐体が不正に開梱された後にその修復が行われた場合であっても、不正な改造が行われたことを確実に知ることができる。

【００３４】従って、カードリーダ装置の装置筐体に対して開梱が行われた場合に、カードリーダ装置そのものの本来動作を不能にすると共に、開梱の後に修復がなされても本来動作の不能状態を継続することによって開梱されたことを当該機器の管理者や正規のカード利用者に知らしめることによってカードの偽造をできなくするというセキュリティ機能付きのカードリーダ装置を提供することができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態によるセキュリティ機能付きのカードリーダ装置の概略回路構成を示すブロック

回路図である。

【図２】図１に示されるセキュリティ機能付きのカードリーダ装置の装置筐体が開梱されたときの動作を説明するためのフローチャートである。

【図３】図２に示すフローチャートの中にあるメッセージの具体例を示す図である。

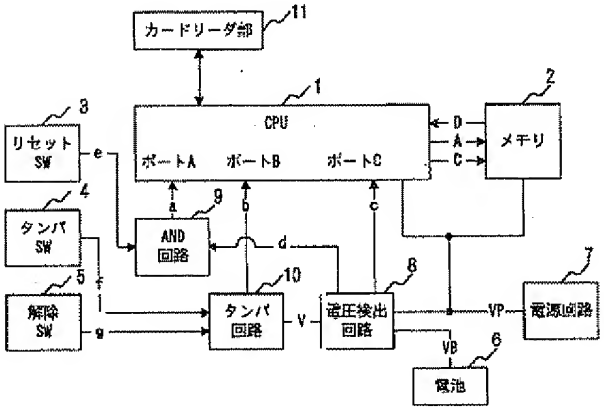
【図４】図１に示されるセキュリティ機能付きのカードリーダ装置の電池が取り外されたときの動作を説明するためのフローチャートである。

【図５】図４に示すフローチャートの中にあるメッセージの具体例を示す図である。

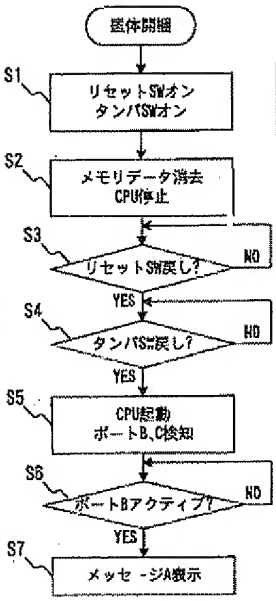
【符号の説明】

１	ＣＰＵ
２	メモリ
３	リセットＳＷ
４	タンパＳＷ
５	解除ＳＷ
６	電池
７	電源回路
８	電源電圧検出回路
９	ＡＮＤ回路
１０	タンパ回路
１１	カードリーダ部

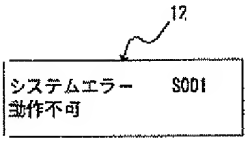
【図１】



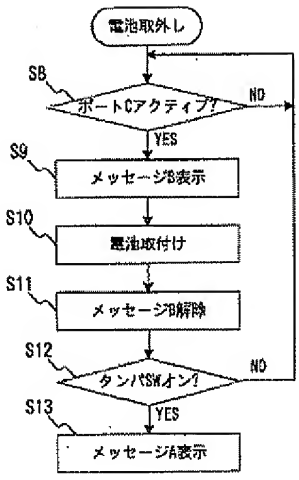
【図２】



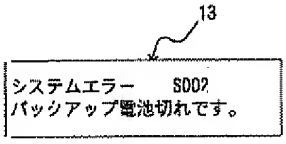
【図３】



【図４】



【図５】



フロントページの続き

Fターム(参考) 2C005 MA02 MA03 MA34 MB08 SA05
SA06 TA24
5B017 AA01 AA07 BA08 BB03 CA14
5B058 CA27 KA02 KA24 KA31 YA20
5B072 AA00 CC02 CC27 CC39 DD04
JJ09 MM09